Office of Science

Program Cyber Security Plan

1.0 Purpose

The purpose of this Plan, the Office of Science Program Cyber Security Plan (PCSP) is to identify the cyber security requirements for the Office of Science (SC) and provide a consistent method to effectively and efficiently oversee and manage work and operations in a manner that ensures the security of information and information systems of all Federal and contractor personnel in accordance with these requirements. In addition, this Plan addresses the implementation of the Federally mandated Certification and Accreditation (C&A) through Cyber Security Program Plans (CSPP) and System Security Plans (SSP) in SC, which include unclassified and national security systems.

2.0 Responsibilities

The following represents the roles and responsibilities of SC managers and staff for Cyber security aspects of their work.

Under Secretary for Science
The Under Secretary for Science is responsible for setting cyber security requirements for the Office of Science and its contractors as set forth in DOE Order 205.1

Director, Office of Science
This senior SC Line Manager is responsible for cyber security performance for the entire Office of Science. As such, the Director of Science is directly accountable to the Under Secretary for Science for the security of information and information systems of Federal and contractor staff. The Director of Science accomplishes this responsibility through further delegations within the organization, as described below.

Chief Operating Officer
Utilizing specific authorities delegated from the Director of Science, the COO is the SC Line Manager responsible and accountable to the Director of Science for the security of information and information systems of Federal and contractor/laboratory staff. The COO routinely communicates with the Director, as well as the Science Information Officer, on all PCSP matters and performance, and develops and implements corrective actions, as appropriate.

Science Information Officer
The Science Information Officer develops SC-specific policies related to cyber security and determines the effectiveness of their control implementation across the SC information systems. Works closely with the COO to represent SC interests regarding the development of cyber security policies, requirements, and initiatives by the Department. Develops, reviews, evaluates, and recommends guidance that supports the

operation of SC facilities. The Science Information Officer is responsible and accountable for developing and maintaining this Plan, its subject areas, and implementation procedures. Interacts with other SC Management Systems (SCMS) MSOs on PCSP issues that interconnect with other SC management systems.

Laboratory Directors
The Laboratory Directors develop, operate, and manage an integrated, ongoing program for cyber security management consistent with the PCSP and lower-tier documents.

Designated Approving Authority
The Designated Approving Authority (DAA) is a senior management official or executive possessing the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. The DAA has inherent U.S. government authority and, as such, must be a government employee. Within SC, the Site Office Manager is the DAA for their laboratory and their own organization; the ISC Manager is the DAA for their location, and the Science Information Officer is the DAA for SC Headquarters.

SC Supervisors
SC Supervisors are responsible for the administrative supervision of Federal and contractor staff assigned to them, including but not limited to: establishing appropriate cyber security standards and behavior in annual employee plans; remedying cyber security deficiencies; assuring performance in accordance with established expectations; and assuring annual security awareness training is provided that reflects current DOE, OMB, National Institute of Standards and Technology (NIST), National Industrial Security Program Operating Manual (NISPOM) (if applicable) policies and guidance. Training must also reflect DOE and SC requirements in policy and CIO Cyber Security Technical and Management Requirements (TMRs).

SC Staff
SC staff (Federal personnel and contractors) is responsible for understanding and complying with PCSP requirements and expectations relevant to their assigned duties, including their own immediate workstation security as well as information systems for which they use and perform administrative duties.

3.0 Plan Operation

3.1 Overview

The Office of Science implements cyber security activities to protect its information and information systems consistent with the principles and functions of NIST and NISPOM. SC staff: 1) ensure that applicable PCSP requirements are followed by SC personnel; 2) ensure that appropriate PCSP requirements are placed into contracts; 3) provide oversight of contractor PCSP work planning and controls; 4) integrate continuous feedback and improvement mechanisms into their work; and 5) perform the necessary oversight and assessments of both the SC contractors and federal staff.

This Plan, also called the PCSP, identifies SC Federal responsibilities and contractor requirements with respect to cyber security. Furthermore, this Plan serves to ensure that SC PCSP requirements and methods of accomplishment are identified, communicated, and implemented by both SC staff and contractors. This includes the oversight, assessment, evaluation of both Federal staff and contractor performance, and reporting of PCSP performance data to SC and other entities (e.g., U.S. Department of Energy [DOE] and, as appropriate, Federal, state, and local governments). Specific processes and criteria for assessing contractor PCSP performance are outlined in the M&O Contract.

3.2 Key Functions/Services and Processes

The PCSP requirements identified in this Plan derive from responsibilities and authorities promulgated to the Undersecretary for Science under DOE Order 205.1A. Further explanation of how SC's Cyber Security Management (CSM) structure establishes a program whereby staff plan, perform, assess, and improve the security of information and information system within the Department of Energy is provided in five, lower-tier documents:

- Continuous Monitoring for Unclassified Systems
- Cyber Security Requirements for Unclassified Systems
- Continuous Monitoring for Classified Systems
- Cyber Security Requirements for Classified Systems
- Designated Approving Authority Responsibilities

Each is discussed briefly below.

3.2.1 Continuous Monitoring for Unclassified Systems

SC is committed to ensuring the proper implementation of PCSP requirements across all its organizations. After a federal information system receive an "Authority to Operate" (ATO), SC is responsible for assuring that controls continue to work as intended and that all changes to the environment are properly documented and analyzed for impact to the organization and mission. SC is also responsible for overseeing that contractors' systems with current ATOs also continue to work as intended and that all changes to their environment are properly documented and analyzed for impact to the organization and its mission. Requirements specific to accomplishing this are provided in the Continuous Monitoring for Unclassified Systems document, which addresses the following subjects:

- Site Review
  - Configuration Management
  - Documentation of Information System Changes
- Metrics
  - SC-wide metrics
  - Site cyber security metrics
- Status Reporting and Documentation
  - Cyber Security Program Plan

- Plan of Action & Milestone update
- Status Reporting

3.2.2 Cyber Security Requirements for Unclassified Systems

SC organizations are expected to implement DOE policy within an SC-directed cyber security framework applicable to their mission and defined by the PCSP and lower-tier documents. The Cyber Security Requirements for Unclassified Systems document identifies the SC application of OCIOs Technical and Management Requirements (TMRs). Specifically, the Cyber Security Requirements for Unclassified Systems document addresses: Federal Laws and Regulations, DOE directives and policies; and SC directives and policies in areas including:

- Protection of Personally Identifiable Information (PII)
- Memorandum of Understanding for interconnected systems
- Contingency Plans
- Access to information systems
- Incident reporting
- Peer to peer networking
- Portable electronic devices
- Plan of Actions and Milestones (POA&M)
- Password management

3.2.3 Continuous Monitoring for Classified Systems

SC is responsible for assuring that cyber security controls relevant to classified systems continue to work as intended, that the trust level of classified systems is maintained, and that all changes to cyber security environment are properly recorded and analyzed for impact to the organization and its mission. Processes and requirements for accomplishing this task are defined in the Continuous Monitoring for Classified Systems document, which includes the following topical areas:

- Site Review
  - Configuration Management
  - Documentation of Information System Changes
- Metrics
  - SC-wide metrics
  - Site cyber security metrics
- Status Reporting and Documentation
  - System Security Plan
  - Plan of Action & Milestone update
  - Status Reporting

3.2.1.4 Cyber Security Requirements for Classified Systems

SC is committed to ensuring that Federal staff performs required Federal program responsibilities in a cost-effective and efficient manner. SC organizations are expected to implement the DOE National Security System Controls Manual within an SC-directed security framework appropriate to the organization's mission. The Cyber Security Requirements for Classified Systems document outlines how SC Federal and contractor staffs implement their PCSP responsibilities related to National Security System control requirements, NIST Special Practice 800-53, Revision 1, high baseline controls, and NISPOM. It includes a discussion on expectations and requirements relating to compliance with: (1) Federal Laws and Regulations: (2) DOE directives: and (3) SC directives and policies, as they pertain to the following:

- Protection of Confidential/Secret/Top Secret information
- Marking of information
- Storage requirements
- Visitation requirements
- Interconnected systems
- Communications security (COMSEC) requirements

3.2.1.5 Designated Approving Authority Responsibilities

FISMA requires that senior (Federal) agency officials assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, modification or destruction of such information or information systems. SC executes this by, among other mechanisms, creating the role of Designated Approval Authority, responsible for ensuring that all the specific Management, Operational, and Technical controls defined in the SC PCSP and lower-tier documents are implemented and work as designed. When this occurs, an organization is granted an Authority to Operate (ATO) by its DAA. SC is responsible for assuring that all DAAs understand their role and the extent of their responsibilities, and these are discussed in this document, which addresses:

- DAA Statutory and regulatory drivers
- Qualifications
- Roles and Responsibilities
- Accreditation and Certification Process
- Authority to Operate
- Important Terms and Definitions

4.0 Requirements

The following lists high-level requirements relevant to this Plan.

P.L. 101-576, Chief Financial Officers (CFOs) Act of 1990, (November 15, 1990)

P.L. 103-356, Government Management Reform Act of 1994, (October 13, 1994)

P.L. 104-13, Paperwork Reduction Act of 1995 (PRA), (May 22, 1995)

P.L. 104-208, Title VIII, Federal Financial Management Improvement Act of 1996 (FFMIA), (October 1, 1996)

P.L. 104-231, Electronic Freedom of Information Act (e-FOIA), (October 2, 1996)

P.L. 105-277, Title XVII, Government Paperwork Elimination Act (GPEA), (October 21, 1998)

P.L. 107-347, Title III, Federal Information Security Management Act of 2002 (FISMA), (December 17, 2002)

P.L. 93-579, Privacy Act of 1974, as amended [Title 5 United States Code (U.S.C.) Section 552a], (December 31, 1974)

P.L. 96-349, Trade Secrets Act - (18 U.S.C., section 1905), (January 22, 2002)

P.L. 97-255, Federal Managers' Financial Integrity Act of 1982 (FMFIA), (September, 8, 1982)

P.L. 99-474, Computer Fraud and Abuse Act (18 U.S.C. section 1030), (October 16.1986)

P.L. 99-508, Electronic Communications Privacy Act of 1986, (October 21, 1986)

P.L. 100-235, Computer Security Act of 1987, (January 8, 1988)

P.L.103-62, Government Performance and Results Act of 1993 (GPRA), (August 3, 1993)

P.L.104-106, Division E, Clinger-Cohen Act (Information Technology Management Reform Act of 1996), (February 10, 1996)

OMB Circular A-11, Planning, Budgeting, Acquisition of Capital Assets, Strategic Plans, Performance Plans, (February 10, 1996)

OMB Circular A-76, Performance of Commercial Activities (Outsourcing), (August 4, 1983)

OMB CircularA-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs, (October 29, 1992)

OMB Circular A-123, Management Accountability and Control, (August 4, 1986), revised (Dec 21, 2004)

OMB Circular A-127, Financial Management Systems, (December 19, 1984) revised (July 23, 1993)

OMB Circular A-130, Management of Federal Information Resources, (June 28, 1993)

OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources, (November 2003)

OMB Memorandum M-95-22, Implementing the Information Dissemination Provisions of the Paperwork Reduction Act of 1995, (September 29, 1995)

OMB Memorandum M-96-20, Implementation of the Information Technology Management Reform Act of 1996, (April 4, 1996)

OMB Memorandum M-97-02, Funding Information Systems Investments, (October 25, 1996)

OMB Memorandum M-97-16, Information Technology Architectures, (June 18, 1997)

OMB Memorandum M-98-04, Annual Performance Plans Required by the Government Performance and Results Act (GPRA), (January 29, 1998)

OMB Memorandum M-99-05, Instructions for Complying With the President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records, (January 7, 1990)

OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, (June 2, 1999)

OMB Memorandum M-99-20, Security of Federal Automated Information Resources, (June 23, 1999)
OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, (February 28, 2000)

OMB Memorandum M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, (April 25, 2000)

OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, (June 22, 2000)

OMB Memorandum M-00-015, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, (September 25, 2000)

OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy, (December 20, 2000)

OMB Memorandum M-01-08, Guidance On Implementing the Government Information Security Reform Act, (January 16, 2001)

OMB Memorandum M-01-26, Component-Level Audits, (July 10, 2001)

OMB Memorandum M-02-12, Reducing Redundant IT Infrastructure to Homeland Security, (July 19, 2002)

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (September 30, 2003)

OMB Memorandum M-04-04, E-Authentication Guidance, (December 16, 2003)

OMB Memorandum M-04-16, Software Acquisition, (July 1, 2004)

OMB Memorandum M-04-25, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, (July 17, 2006)

OMB Memorandum M-04-26, Personal Use Policies and "File Sharing" Technology, (September 8, 2004)

OMB Memorandum M-05-02, Financial Management Systems, (December 1, 2004)

OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, (December 17, 2004)

OMB Memorandum M-05-05, Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services, (December 20, 2004)

OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, (February 11, 2005)

OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, (May 22, 2006)

OMB Memorandum M-06-16, Protection of Sensitive Agency Information, (June 23, 2006)

OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments, (July 12, 2006)

NIST Federal Information Processing Standard (FIPS) 201-1, National Institute of Standards and Technology (NIST) Personal Identity Verification (PIV) of Federal Employees and Contractors, (March 2006)

NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (March 2006)

NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, (February 2004)

NIST FIPS 142-2, Security requirements for Cryptographic Modules, (May 2001)

NIST Special Publication (SP) 800-92, Guide to Computer Security Log Management, (September 2006)

NIST SP 800-88, Guidelines for Media Sanitization, (September 2006)

NIST SP 800-83, Guide to Malware Incident Prevention and Handling, (November 2005)

NIST SP 800-73, Rev. 1, Interfaces for Personal Identity Verification, March 2006, (updated April 20, 2006)
.
NIST SP 800-70, The NIST Security Configuration Checklists Program, (May 2005)

NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Process, (January 2005)

NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, Revision 1, (June 2004)

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, (June 2004)

NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, (April 2006)

NIST SP 800-53, Rev. 1, Recommended Security Controls for Federal Information Systems, (December 2006)

NIST SP 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, (November 2002)

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, (May 2004)

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, (June 2002)

NIST SP 800-30, Risk Management Guide for Information Technology Systems, (July 2002)

NIST SP 800-26, Rev. 1, Guide for Information Security Program Assessments and System Reporting Form, (November 2001)

NIST SP 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems, (February 2006)

DOE 0 142.3, Unclassified Foreign Visits and Assignments, (June18, 2004)

DOE P 205.1, Departmental Cyber Security Management Policy, (May 8, 2001)

DOE O 205.1A, Department of Energy Cyber Security Management Program, (December 4, 2006)

DOE 0 221.1, Reporting Fraud, Waste, and Abuse to the Office of Inspector General, (April 22, 2001)

DOE 0 221.2, Cooperation with the Office of Inspector General, (March 22, 2001)

DOE P 226.1, Department of Energy Oversight Policy, (June 10, 2005)

DOE 0 226.1, Implementation of Department of Energy Oversight Policy, (September 15, 2005)

DOE N 221.11, Reporting Fraud, Waste, and Abuse, (September 20, 2005)

DOE P 470.1, Integrated Safeguards and Security Management (ISSM) Policy, (May 8, 2001)

DOE 0 470.2B, Independent Oversight and Performance Assurance Program, (October 31, 2002)

DOE 0 471.1, Identification and Protection of Unclassified Controlled Nuclear Information, (June 30, 2000)

DOE 0 470.4, Safeguards and Security Program, (August 26, 2005)

DOE 0 475.1, Counterintelligence Program, *(*February 10, 2004)

E.O. 12344, Naval Nuclear Propulsion Program, (February 1, 1982)

E.O. 12958, Classified National Security Information, (April 17, 1995)

E.O. 13011, Federal Information Technology, (July 17, 1996)

E.O. 13231, Critical Infrastructure Protection in the Information Age, (October 16, 2001)

E.O. 13228, Establishing the Office of Homeland Security and the Homeland Security Council, (October 8, 2001)

Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, (December 17, 2003)

HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, (August 27, 2004)

National Security Directive (NSD) 42, National Policy for the Security of National Security Telecommunications and Information Systems, (October 5, 1989)

NSTISSC Policy No.11, Issuances of the Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC),] National Information Assurance Acquisition Policy, (July 2003)

NSTISSC Directive No. 500, Information Systems Security (INFOSEC) Education, Training, and Awareness, (February 25, 1993)

NSTISSC Directive No. 501, National Training Program for Information Systems Security (INFOSEC) Professionals, (November 16, 1992)

NSTISSC INFOSEC 1-99, The Insider Threat to U S. Government Information Systems, (July 1999)

Instruction No. 1000, National Information Assurance Certification and Accreditation Process, (April 2000)

NISPOM, National Industrial Security Program Operations Manual, (February 2006)

5.0 Subject Areas

None

6.0 References

The following summarizes high-level references relevant to this Plan.

OMB Circular A-11, Planning, Budgeting, Acquisition of Capital Assets, Strategic Plans, Performance Plans, (February 10, 1996)

OMB Circular A-76, Performance of Commercial Activities (Outsourcing), (August 4, 1983)

OMB Circular A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs, (October 29, 1992)

OMB Circular A-123, Management Accountability and Control, (August 4, 1986), revised (December 21, 2004)

OMB Circular A-127, Financial Management Systems, (December 19, 1984), revised (July 23, 1993)

OMB Circular A-130, Management of Federal Information Resources, (June 28, 1993)

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, (November 2003)

OMB Memorandum M-95-22, Implementing the Information Dissemination Provisions of the Paperwork Reduction Act of 1995, (September 29, 1995)

OMB Memorandum M-96-20, Implementation of the Information Technology Management Reform Act of 1996, (April 4, 1996)

OMB Memorandum M-97-02, Funding Information Systems Investments, (October 25, 1996)

OMB Memorandum M-97-16, Information Technology Architectures, (June 18, 1997)

OMB Memorandum M-98-04, Annual Performance Plans Required by the Government Performance and Results Act (GPRA), (January 29, 1998)

OMB Memorandum M-99-05, Instructions for Complying With the President's Memorandum of May 14, 1998, “Privacy and Personal Information in Federal Records”, (January 7, 1990)

OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, (June 2, 1999)

OMB Memorandum M-99-20, Security of Federal Automated Information Resources, (June 23, 1999)

OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, (February 28, 2000)

OMB Memorandum M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, (April 25, 2000)

OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, (June 22, 2000)

OMB Memorandum M-00-015, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, (September 25, 2000)

OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy, (December 20, 2000)

OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, (January 16, 2001)

OMB Memorandum M-01-26, Component-Level Audits, (July 10, 2001)

OMB Memorandum M-02-12, Reducing Redundant IT Infrastructure to Homeland Security, (July 19, 2002)

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (September 30, 2003)

OMB Memorandum M-04-04, E-Authentication Guidance, (December 16, 2003)

OMB Memorandum M-04-16, Software Acquisition, (July 1, 2004)

OMB Memorandum M-04-25, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, (July 17, 2006)

OMB Memorandum M-04-26, Personal Use Policies and "File Sharing" Technology, (September 8, 2004)

OMB Memorandum M-05-02, Financial Management Systems, (December 1, 2004)

OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, (December 17, 2004)

OMB Memorandum M-05-05, Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services, (December 20, 2004)

OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, (February 11, 2005)

OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, (May 22, 2006)

OMB Memorandum M-06-16, Protection of Sensitive Agency Information, (June 23, 2006)

OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments", (July 12, 2006)

NIST Federal Information Processing Standard (FIPS) 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, (March 2006)

NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (March 2006)

NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, (February 2004)

NIST FIPS 142-2, Security requirements for Cryptographic Modules, (May 2001)

NIST Special Publication (SP) 800-92, Guide to Computer Security Log Management, (September 2006)

NIST SP 800-88, Guidelines for Media Sanitization, (September 2006)

NIST SP 800-83, Guide to Malware Incident Prevention and Handling, (November 2005)

NIST SP 800-73, Rev. 1, Interfaces for Personal Identity Verification, March 2006, (updated April 20, 2006)

NIST SP 800-70, The NIST Security Configuration Checklists Program, (May 2005)

NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Process, (January 2005)

NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, Revision 1, (June 2004)

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, (June 2004)110

NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, (April 2006)

NIST SP 800-53, Rev. 1, Recommended Security Controls for Federal Information Systems, (December 2006)

NIST SP 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, (November 2002)

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, (May 2004)

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, (June 2002)

NIST SP 800-30, Risk Management Guide for Information Technology Systems, (July 2002)

NIST SP 800-26, Rev. 1, Guide for Information Security Program Assessments and System Reporting Form, (November 2001)

NIST SP 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems, (February 2006)

DOE Chief Information Officer Guidance – Cyber Security

CS-01, Controls for Unclassified Systems, (June 30, 2006)

CS-02, Certification and Accreditation, (March 24, 2006)

CS-03, Risk Management, (June 30, 2006)

CS-04, Vulnerability Management, (July 31, 2006)

CS-05, Interconnect Agreements, (July 31, 2006)

CS-06, Plans of Actions and Milestones (POA&M), (September 07, 2006)

CS-07, Contingency Planning, (August 26, 2006)

CS-08, Configuration Management, (November 27, 2006)

CS-09, Incident Management, (January 2007)

CS-11, Clearing and Media Sanitization (January 2007)

CS-12, Password Management, (June 30, 2006)

CS-13, Wireless Devices and Information Systems, (June 30, 2006)

CS-14, Portable/Mobile Devices (January 2007)

CS-15, Personally Owned Devices (January 2007)

CS-20, INFOCON, (December 06, 2006)

CS-23, Peer-To Peer Networking (December 2006)

CS-24, Remote Access (January 2007)

CS-37, Security, Testing and Evaluation (January 2007)

CS-38A, Protection of Sensitive Unclassified Information, including Personally Identifiable Information (November 2006)

NSTISSC Policy No.11, National Information Assurance Acquisition Policy, (July 2003)

NSTISSC Directive No. 500, Information Systems Security (INFOSEC) Education, Training, and Awareness, (February 25, 1993)

NSTISSC Directive No 501, National Training Program for Information Systems Security (INFOSEC) Professionals, (November 16, 1992)

NSTISSC INFOSEC 1-99, The Insider Threat to U S. Government Information Systems, (July 1999)

Instruction No. 1000, National Information Assurance Certification and Accreditation Process, (April 2000)

NISPOM, National Industrial Security Program Operations Manual, (February 2006)